Câu 1: Hãy trình bày các giao thức thực hiện bảo mật, cách thức bảo vệ hệ thống khỏi sự xâm nhập và phá hoại từ bên ngoài.

Gợi ý: trình bày các giao thức thực hiện bảo mật (Keberos, X509, SSL, PGP và S/MIME, IPSET).

Kerberos là gì?

Kerberos là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn. Giao thức Kerberos có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu. Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình client - server và đảm bảo xác thực cho cả hai chiều.

Giao thức được xây dựng dựa trên mã hoá đối xứng và cần đến một bên thứ ba mà cả hai phía tham gia giao dịch tin tưởng.

X, 509 là một định dạng chuẩn cho **chứng chỉ khóa công khai**, các tài liệu kỹ thuật số liên kết an toàn các cặp khóa mật mã với các danh tính như trang web, cá nhân hoặc tổ chức.

Các ứng dụng phổ biến của chứng chỉ X.509 bao gồm:

- SSL /TLS và HTTPS để duyệt web xác thực và mã hóa
- Email đã ký và được mã hóa thông qua S/MIME giao thức
- Ký mã
- Ký văn bản
- Xác thực ứng dụng khách
- ID điện tử do chính phủ cấp

Các ứng dụng phổ biến của chứng chỉ X.509 bao gồm SSL /TLS và HTTPS để duyệt web được xác thực và mã hóa, email đã ký và mã hóa qua S/MIME giao thức, ký mã, ký văn bản, xác thực khách hàngvà ID điện tử do chính phủ cấp.

SSL là chữ viết tắt của Secure Sockets Layer là giao thức mã hóa dữ liệu được truyền tải từ máy khách đến server Hosting và ngược lại thông qua trình duyệt. Tất cả dữ liệu truyền điều được mã hóa. SSL CHỈ có tác dụng BẢO MẬT ĐƯỜNG TRUYỀN DỮ LIỆU (Bảo mật các gói tin được gửi đi trong quá trình vận chuyển - tránh việc chặn gói

tin và giải mã chúng khi đang vận chuyển) chứ **không phải cứ có SSL là website của Bạn không bị hack**.

Xác thực website, giao dịch.
Nâng cao hình ảnh, thương hiệu và uy tín doanh nghiệp.
Bảo mật các giao dịch giữa khách hàng và doanh nghiệp, các dịch vụ truy nhập hệ thống.
Bảo mật webmail và các ứng dụng như Outlook Web Access, Exchange, và Office Communication Server.
Bảo mật các ứng dụng ảo hó như Citrix Delivery Platform hoặc các ứng dụng điện toán đám mây.
Bảo mật dịch vụ FTP.
Bảo mật truy cập control panel.
Bảo mật các dịch vụ truyền dữ liệu trong mạng nội bộ, file sharing, extranet.
Bảo mật VPN Access Servers, Citrix Access Gateway …

Mã hóa PGP (Pretty Good Privacy) là một hệ thống được sử dụng cho việc mã hóa email và mã hóa các file nhạy cảm.

Cách hoạt động:

Đầu tiên, PGP tạo session key ngẫu nhiên bằng cách sử dụng một trong hai thuật toán chính. Key này là một con số khổng lồ không thể đoán được, và chỉ được sử dụng một lần.

• Tiếp theo, session key này được mã hóa. Điều này được thực hiện bằng cách sử dụng public key của người nhận thư. Public key gắn liền với danh tính của một người cụ thể và bất kỳ ai cũng có thể sử dụng key này để gửi tin nhắn cho họ.

• Người gửi sẽ gửi PGP session key được mã hóa của họ cho người nhận và họ có thể giải mã bằng private key của họ. Sử dụng session key này, người nhận bây giờ có thể giải mã tin nhắn.

IP Security (IPSec – Internet Protocol Security) là một giao thức được chuẩn hoá bởi IETF (Internet Engineering Task Force) từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Hay nói cách khác, IPSec là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cẩn mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thiết bị mạng.

IPSEC

- Bảo vệ kết nối từ các mạng chi nhánh đến mạng trung tâm thông qua Internet.
- Bảo vệ kết nối truy cập từ xa (Remote Access).
- Thiết lập các kết nối Intranet và Extranet .
- Nâng cao tính bảo mật của các giao dịch thương mại điện tử.

1.2.1 Ưu điểm

- Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng, thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan đến bảo mật.
- IPSec được thực hiện bên dưới lớp TCP và UDP, đồng thời nó hoạt động trong suốt đối với các lớp này. Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
- IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối, điều này giúp che giấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua mạng Internet.

1.2.2 Hạn chế

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

Đa dụng Internet Mail Extension (S / MIME) là một bảo vệ nâng cấp lên tiêu chuẩn định dạng e-mail Internet MIME dựa trên công nghệ của RSA Data Security

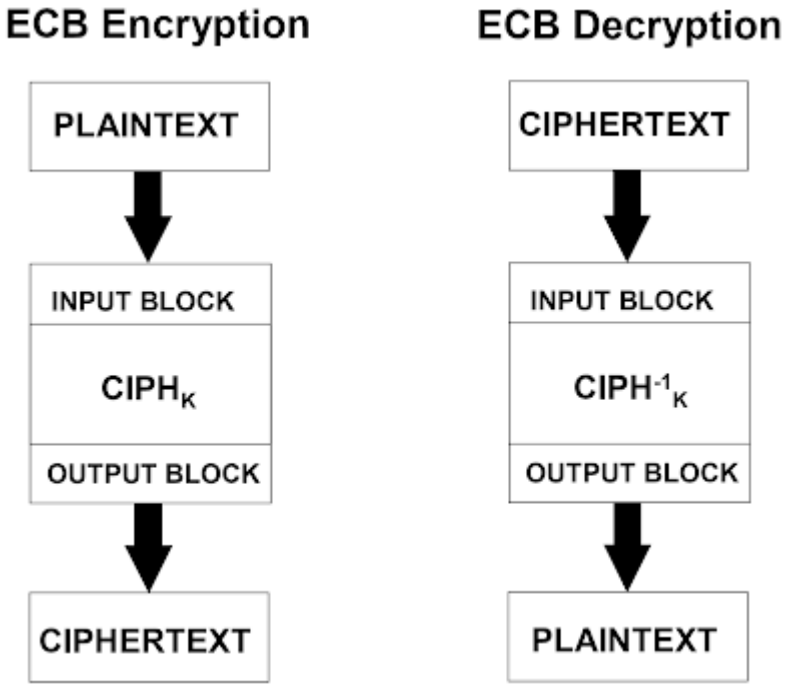
Cách thức bảo về hệ thống

Các thức bảo vệ: khái niệm Control Access (kiểm soát truy cập) dùng cho việc bảo vệ này (chứng thực và phân quyền), đồng thời sử dụng Firewall hoặc các hệ thống phát hiện chống xâm nhập IDS/IPS, kiểm lỗi phần mềm.

Câu 2: Trình bằng mô hình mã và giải mã khối Electronic Codebook – ECB, những ưu điểm và nhược điểm của ECB, CBC, CFB, OFB, CTR.

ECB (Electronic Codebook)

ECB là chế độ mã hóa từng khối bit độc lập. Với cùng một khóa mã K, mỗi khối plaintext ứng với một giá trị ciphertext cố định và ngược lại.



Ưu điểm:

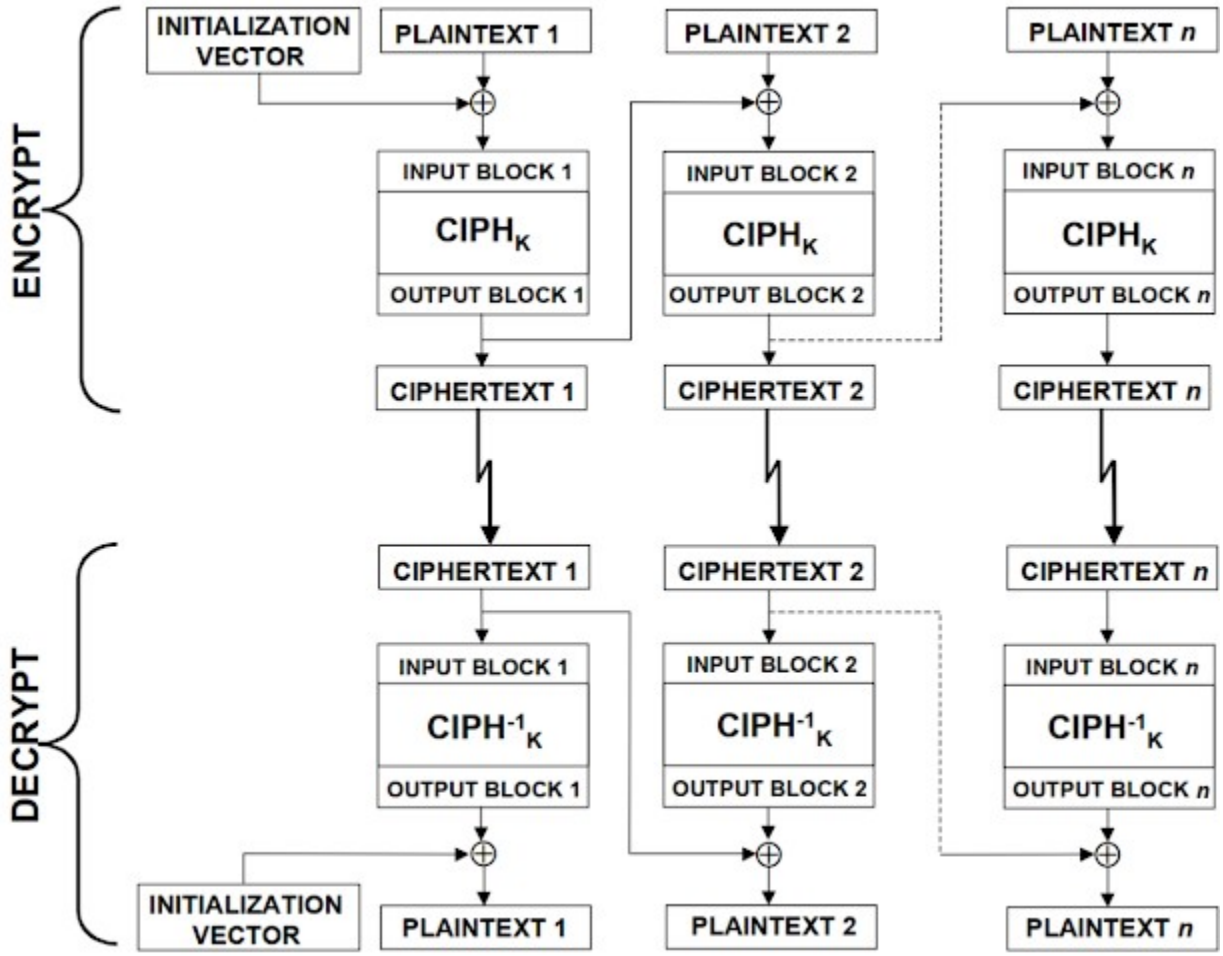
- *Đơn giản*
- *Không cần đồng bộ hóa giữa bên gửi và nhận, nếu bên nhận không nhận đủ các khối, thì vẫn có thể giải mã các khối nhận được.*

- *Các bit lỗi sẽ không được đưa vào các khối kế sau.*
- *Vì các khối được mã hóa và giải mã hoàn toàn độc lập với nhau nên ECB cho phép mã hóa và giải mã đồng thời nhiều khối nếu có đủ phần cứng thực thi.*

Nhược điểm:

- *ECB về bản chất giống hệt với các mật mã bảng chữ cái cổ điển, chỉ có điều bảng chữ cái của ECB phức tạp hơn.*
- *Các khối bản rõ giống nhau sẽ được ánh xạ thành khối bản mã giống nhau (nếu dùng cùng 1 loại khóa), dẫn đến dễ tấn công bằng phương pháp thống kê tần suất.*
- *ECB dễ dàng bị phá nếu bản rõ lớn và có tính cấu trúc rõ ràng, từ đó ECB thường dùng để mã hóa những bản rõ ngắn như khóa bí mật.*
- *ECB song song hóa được, có cấu trúc quy luật -> độ an toàn yếu.*

CBC là chế độ mã hóa chuỗi, kết quả mã hóa của khối dữ liệu trước (ciphertext) sẽ được tổ hợp với khối dữ liệu kế tiếp (plaintext) trước khi thực thi mã hóa.



Ưu điểm:

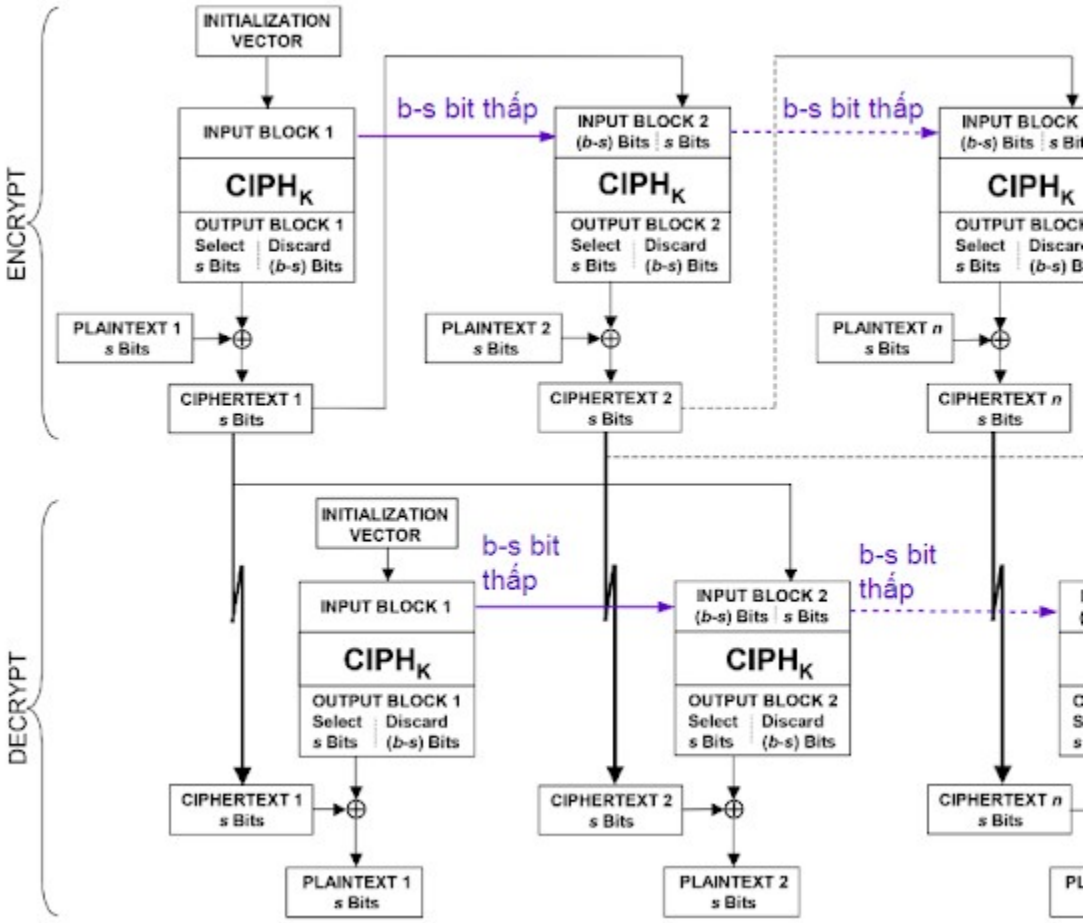
- Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào ***IV*** hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
- Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.

Nhược điểm:

- Thiết kế phần cứng phức tạp hơn ECB ngoài logic thực thi thuật toán mã hóa, người thiết kế cần thiết kế thêm:
- Logic quản lý độ dài chuỗi dữ liệu sẽ được mã hóa, cụ thể là số lượng khối dữ liệu trong chuỗi dữ liệu.
- Bộ tạo giá trị ngẫu nhiên cho ***IV***.
- Lỗi bit bị lan truyền. Nếu một lỗi bit xuất hiện trên ciphertext của một khối dữ liệu thì nó sẽ làm sai kết quả giải mã của khối đữ liệu đó và khối dữ liệu tiếp theo.

- Không thể thực thi quá trình mã hóa song song vì xử lý của khối dữ liệu sau phụ thuộc vào ciphertext của khối dữ liệu trước, trừ lần mã hóa đầu tiên.

CFB là chế độ mã hóa mà ciphertext của lần mã hóa hiện tại sẽ được phản hồi (feedback) đến đầu vào của lần mã hóa tiếp theo. Nghĩa là, ciphertext của lần mã hóa hiện tại sẽ được sử dụng để tính toán ciphertext của lần mã hóa kế tiếp. Mô tả có vẻ giống CBC nhưng quá trình trực hiện lại khác.



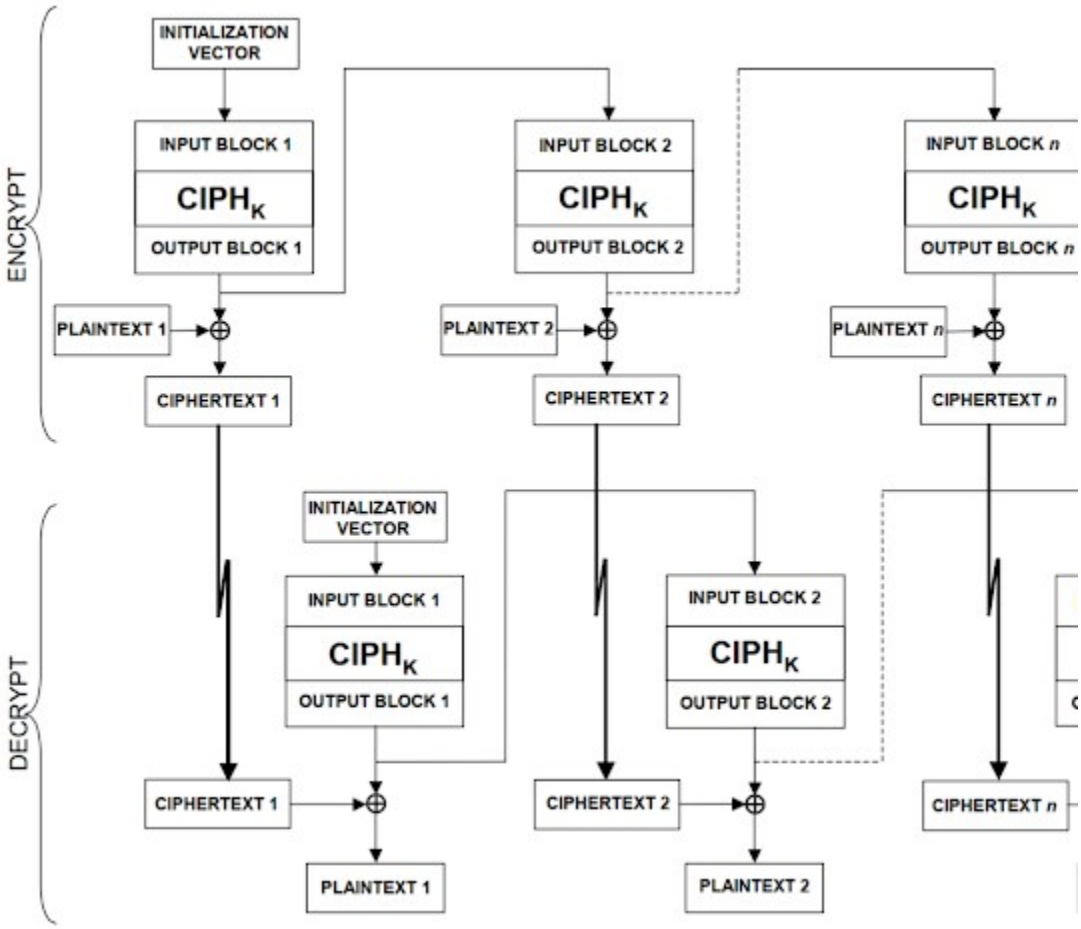
Ưu điểm:

- Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào **IV** hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
- Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.
- Tùy biến được độ dài khối dữ liệu mã hóa, giải mã thông qua thông số **s**

Nhược điểm:

- Thiết kế phần cứng phức tạp hơn CBC. Ngoài những thành phần logic như CBC, CFB cần thêm logic để chọn số bit cần được xử lý nếu **s** là thông số cấu hình được.
- Lỗi bit bị lan truyền. Nếu một lỗi bit xuất hiện trên ciphertext của một khối dữ liệu thì nó sẽ làm sai kết quả giải mã của khối đữ liệu đó và khối dữ liệu tiếp theo.
- Không thể thực thi quá trình mã hóa song song vì xử lý của khối dữ liệu sau phụ thuộc vào ciphertext của khối dữ liệu trước, trừ lần mã hóa đầu tiên

OFB là chế độ mã hóa mà giá trị ngõ ra của khối thực thi thuật toán mã hóa, **không phải ciphertext**, của lần mã hóa hiện tại sẽ được phản hồi (feedback) đến ngõ vào của lần mã hóa kế tiếp.

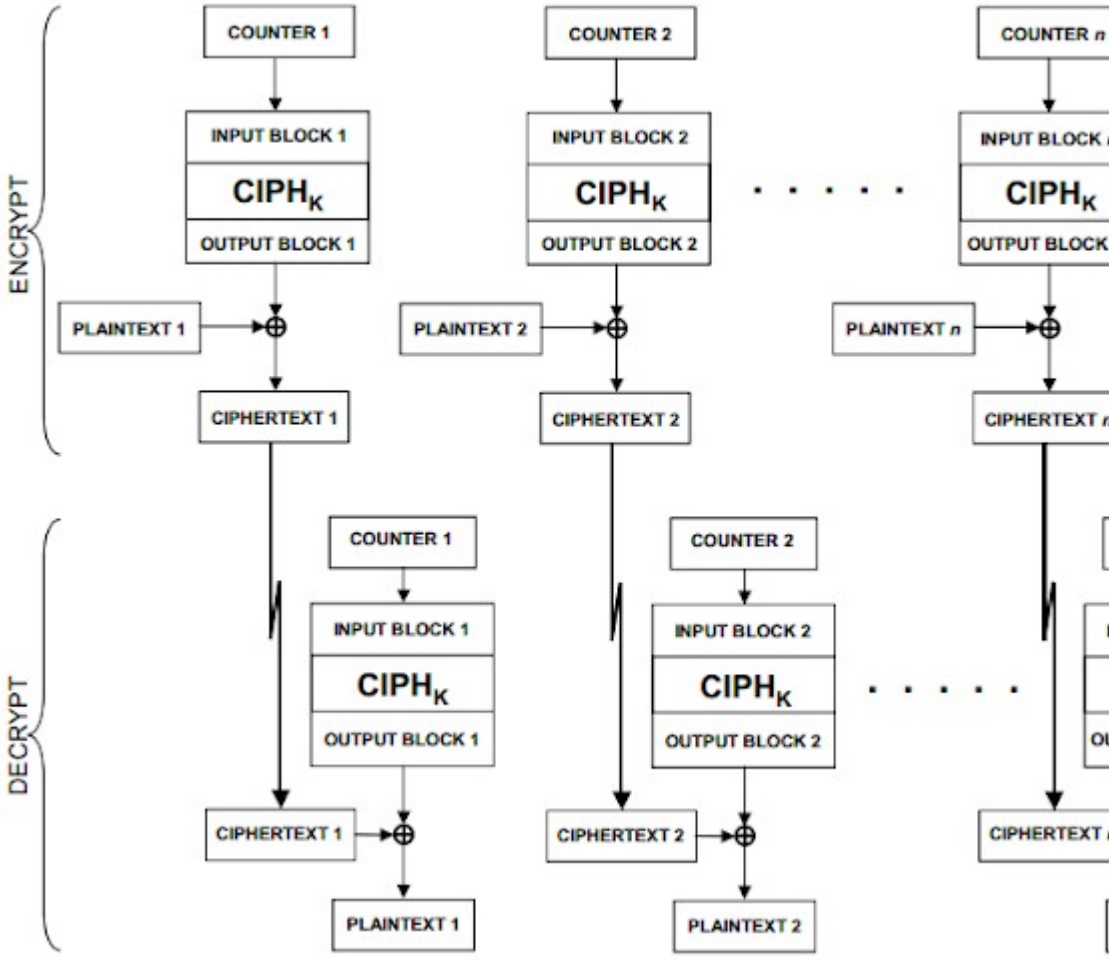


Ưu điểm:

Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext

có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào **IV** hoặc khối ngõ ra của lần mã hóa trước đó.
Lỗi bit không bị lan truyền. Khi một lỗi bit xuất hiện trên một ciphertext, nó chỉ ảnh hưởng đến kết quả giải mã của khối dữ liệu hiện tại
Thiết kế phần cứng đơn giản hơn CFB.
Nhược điểm:
Không thể thực hiện mã hóa/giải mã song song nhiều khối dữ liệu vì lần mã hóa/giải mã sau phụ thuộc vào khối ngõ ra của lần mã hóa/giải mã liền trước nó.

CTR là chế độ mã hóa sử dụng một tập các khối ngõ vào, gọi là các counter, để sinh ra một tập các giá trị ngõ ra thông qua một thuật toán mã hóa. Sau đó, giá trị ngõ ra sẽ được XOR với plaintext để tạo ra ciphertext trong quá trình mã hóa, hoặc XOR với ciphertext để tạo ra plaintext trong quá trình giải mã.



Ưu điểm:
Khả năng bảo mật cao hơn ECB. Tuy quá trình mã hóa/giải mã của mỗi khối dữ liệu là độc lập nhưng mỗi plaintext có thể ảnh xạ đến nhiều ciphertext tùy vào giá trị bộ đếm của các lần mã hóa.
Có thể mã hóa/giải mã song song nhiều khối dữ liệu.
Nhược điểm:
Phần cứng cần thiết kế thêm các bộ đếm counter hoặc giải thuật tạo các giá trị counter không lặp lại.

- *Thay đổi thông điệp*
- *Mạo danh*
- *Phát lại thông điệp*
- *Ngăn chăn thông tin*

Câu 4: Hãy trình bày các yêu cầu của một hệ thống truyền thông tin an toàn và bảo mật, cho biết vai trò của mật mã học trong việc bảo vệ thông tin trên mạng.

Gợi ý:

Tính bí mật (Confidentiality): bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép.

Tính toàn vẹn (Integrity): Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.

Tính sẵn sàng (Availability): Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu

Tính chống thoái thác (Non-repudiation): Khả năng ngăn chặn việc từ chối một hành vi đã làm

Vai trò: Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin. Mật mã đáp ứng được các dịch vụ như xác

thực, bảo mật, toàn vẹn dữ liệu, chống chối bỏ

Câu 10: Nêu nhược điểm của mã hóa khóa công khai?

Nhược điểm của mã hóa đối xứng:

– Vấn đề trao đổi khóa giữa người gửi và người nhận: Phải truyền khóa trên kênh an toàn để giữ bí mật. Ngay nay điều này tỏ ra không hợp lý vì khối lượng thông tin luân chuyển trên khắp thế giới là rất lớn.

– Tính bí mật của khóa (Tính không từ chối): Vì khóa 2 người dùng chung nên khi khóa bị lộ không có cơ sở quy trách nhiệm cho ai.

Câu 11: Trình bày quá trình tạo khóa và mã hóa của RSA ?

Nếu chúng ta có bản rõ M, chúng ta cần chuyển nó thành một số tự nhiên m trong khoảng (0, n) sao cho m, n nguyên tố cùng nhau. Việc này rất dễ dàng thực hiện bằng cách thêm một các kỹ thuật padding. Tiếp theo, chúng ta sẽ má hóa m, thành c như sau:

Sau đó giá trị c sẽ được chuyển cho người nhận.

Ở phía người nhận, họ sẽ giải mã từ c để lấy được m như sau:

Từ m có thể lấy lại được bản tin bằng cách đảo ngược padding

Cụ thể, khóa của RSA được sinh như sau:

- Chọn 2 số nguyên tố p và q
- Tính n = pq. Sau này, n sẽ được dùng làm modulus trong cả public key và private key.

- Tính một số giả nguyên tố bằng phi hàm Carmichael như sau: $\lambda(n) = BCNN(\lambda(p), \lambda(q)) = BCNN(p - 1, q - 1)$. Giá trị này sẽ được giữ bí mật.
- Chọn một số tự nhiên e trong khoảng $(1, \lambda(n))$ sao cho $ƯCLN(e, \lambda(n)) = 1$, tức là e và $\lambda(n)$ nguyên tố cùng nhau.
- Tính toán số d sao cho $d \equiv 1/e \pmod{\lambda(n)}$ hay viết dễ hiểu hơn thì $de \equiv 1 \pmod{\lambda(n)}$. Số d được gọi là số nghịch đảo modulo của e (theo modulo $\mod \lambda(n)$).

Câu 12: Trình bày các giải pháp trao đổi khóa công khai? Cho biết hoàn cảnh áp dụng từng giải pháp?

Trao đổi khóa Diffie-Hellman là một trong những phát triển quan trọng nhất trong mật mã khóa công khai và nó vẫn được thực hiện thường xuyên trong một loạt các giao thức bảo mật khác nhau ngày nay.

Nó cho phép hai bên trước đây chưa gặp nhau thiết lập một cách an toàn một khóa mà họ có thể sử dụng để bảo mật thông tin liên lạc của họ.

Mục đích chính của trao đổi khóa Diffie-Hellman là để phát triển an toàn các bí mật được chia sẻ có thể được sử dụng để lấy khóa. Các khóa này sau đó có thể được sử dụng với các thuật toán khóa đối xứng để truyền thông tin theo cách được bảo vệ. Các thuật toán đối xứng có xu hướng được sử dụng để mã hóa phần lớn dữ liệu vì chúng hiệu quả hơn các thuật toán khóa công khai.

Là một trong những phương pháp phổ biến nhất để phân phối khóa an toàn, trao đổi khóa Diffie-Hellman là thường xuyên được thực hiện trong các giao thức bảo mật như TLS, IPsec, SSH, PGP và nhiều giao thức khác.

Câu 13: Giải thích tính an toàn của giải pháp trao đổi khóa bí mật sử dụng hệ mã hóa công khai ?

Hệ mã công khai sử dụng hai khóa có quan hệ toán học với nhau, tức là một khóa này được hình thành từ khóa kia: Người muốn nhận bản mã (Alice) tạo ra một khóa mật (private key) và từ khóa mật tính ra khóa công khai (public key) với một thủ tục không phức tạp, còn việc tìm khóa mật khi biết khóa công khai là bài toán khó giải được. Khóa công khai sẽ đưa đến cho người gởi bản tin (Bob) qua kênh công cộng. Và bản tin được Bob mã hóa bằng khóa công cộng.

Bản mã truyền đến Alice, và nó được giải mã bằng khóa mật.

Câu 15: Phương pháp hoán vị dùng nguyên tắc gì để mã hóa?

Về bản chất thì kỹ thuật hoán vị chỗ chính là trường hợp đặc biệt của kỹ thuật thay thế. Trong kỹ thuật này, tập hợp các ký tự của bản nguồn sẽ không thay đổi so với bản mã mà chỉ thay đổi vị trí của các ký tự.